



Federal Bureau of Investigation
Pittsburgh CART

Charleston, WV, Resident Agency
113 Virginia Street East
Charleston, WV 25301

REPORT OF EXAMINATION

To: Pittsburgh
Charleston, WV RA
SA Jared Jankowski

Date: November 30, 2022
Case ID: 305D-PG-3501933
Request No.: 270118

Request Date: August 24, 2022

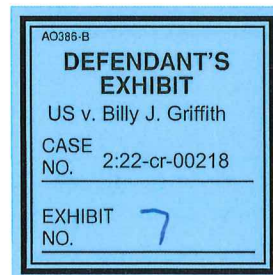
Ref. No.: N/A

Title: Billy Griffith; Saint Albans, WV; Possession of Child Pornography

Date item(s) received: August 24, 2022

Item(s) Submitted (this report will only cover the following items):

Item02	1B2, E01774118	Samsung mobile device, Model SM-T510, Serial Number (S/N) R5210V705X
Item07	1B7, E6999253	Seagate hard drive, Model ST5000DM002, S/N S2ABSTRW
Item08	1B8, E6999254	Seagate hard drive, Model ST31000528AS, S/N 9VP6WVVT
Item14	1B14, E6999260	Samsung mobile device, Model SM-G970U (Galaxy S10e), S/N R58M34SKCKW, International Mobile Equipment Identity (IMEI) 352066102864183
Item17	1B17, E6998881	LG mobile device, Model LM-V600 (V60 ThinQ 5G), IMEI 353271112019922, S/N 008KPLC0121792
Item21	1B21, E6999267	Samsung mobile device, Model SM-G935A (Galaxy S7 edge), S/N R38H30ZQP4P; IMEI 355503071207538; containing Subscriber Identity Module (SIM) Card Integrated Circuit Card ID (ICCID) 89014104271474364335
Item24	1B24, E6999270	Dell laptop computer, Model Inspiron 3542, S/N 8ZQZ532
Item24_1		HGST hard drive, Model HTS547575A9E384, S/N 130914J21400K4KV4N1B
Item25	1B25, E6999271	CyberPower desktop computer, Model C Series
Item25_1		Western Digital SATA SSD, Model WDS240G2G1A, S/N 202014A00DAD
Item25_2		Seagate hard drive, Model ST1000DM010, S/N ZN1JLLN3



Summary:

Special Agent (SA) Jared Jankowski requested a Computer Analysis Response Team (CART) certified examiner process requested items for evidence of Child Sexual Abuse Material (CSAM). This request was made pursuant to a Search Warrant issued by the United States District Court for the Southern District of West Virginia.

An advanced method was used to extract data from Item02 (Samsung SM-T510) . The extractions were then processed and a digital report was provided for review. The digital report was preserved on a Blu-Ray disc labeled DEPG03.

Item07 (Seagate hard drive, Model ST5000DM002, S/N S2ABSTRW) was damaged and could not be accessed. A request was submitted to Operational Technology Division – Digital Forensic Analysis Unit – Mission Support and Data Recovery Program (MSDRP). MSDRP advised that the drive had extensive physical damage to the platters and no data could be recovered.

A forensic image was created of Item08 (Seagate hard drive, Model ST31000528AS, S/N 9VP6WVVT). The image was then processed and categorized. A review was conducted for evidence of CSAM. A total of 74 files and 97 thumbnails were labeled as Child Exploitation and/or CSAM. These files were exported and placed on a Compact Disc (CD) labeled DEPG04.

An advanced method was used to extract data from Item14 (Samsung Galaxy S10e). The extractions were then processed and a digital report was provided for review. The digital report was preserved on a forensically clean 128 GB SanDisk thumb drive labeled DEPG01.

Item17 (LG V60 ThinQ 5G) was locked with an unknown pattern lock. Attempts to bypass the lock were unsuccessful. A request was made to Electronic Device Analysis Unit for assistance. As of this date, the request is pending.

An advanced method was used to extract data from Item21 (Galaxy S7 Edge). The extractions were then processed and a digital report was provided for review. The digital report was preserved on a Blu-Ray disc labeled DEPG02.

Seven (7) files were marked as possible child exploitation. These files were found in userdata (ExtX)/Root/data/com.google.android.gms/files/downloads/.

A forensic image was created of the HGST hard drive contained within Item24 (Dell laptop). The image was then processed and categorized. A review was conducted for evidence of CSAM. A total of 341 files and 1,820 thumbnails were labeled as Child Exploitation and/or CSAM. These files were exported and placed on a Compact Disc (CD) labeled DEPG05.

Screenshots of what appear to be a Samsung device were located on this computer. Multiple applications indicating the use of file sharing and/or torrent browsers were noted. These applications include DropBox, Frostwire, One Drive, Onion Browser, TorBrowser, WeTorrent, Orbot and Orweb. Applications indicating wiping/erasing were also noted.

305D-PG-3501933

270118

Page 2 of 14

GRIFFITH-000224

These include Secure Eraser and SecureWipe. Applications indicating advanced file access were also noted. These include DiskDigger, FileChef and Recover Deleted Data. In addition, applications with file sharing features were noted. These include Discord, MeWe, My Cloud OS 3, Signal, Snapchat, TextFree, Twitter, Facebook Messenger, Facebook Messenger Kids and Zello.

Artifacts identifying DropBox were identified. However, no user data could be identified. Artifacts identifying OneDrive were also identified. A OneDrive account for "bugman25177@gmail.com" was identified.

A forensic image was created of both the Western Digital hard drive and the Seagate hard drive contained within Item25 (CyberPower desktop). The images were then processed and categorized. A review was conducted for evidence of CSAM. The Seagate hard drive appeared to be unused and was not examined further. From the Western Digital hard drive, a total of 21,774 thumbnails were labeled as Child Exploitation and/or CSAM. These files were exported and placed on a Compact Disc (CD) labeled DEPG06.

The image files were archived to an LTO6 cartridge labeled DEPG06. A copy of the examination results and processing were archived to an LTO5 cartridge labeled DEPG08.

Details of Examination:

This examination was conducted between August 24, 2022, and November 28, 2022.

Item02 – Samsung mobile device, Model SM-T510, S/N R5210V705X

The following processes were performed:

- Reviewed legal authority
- Isolated device
- Physically examined device
- Extracted data from device with advanced method
- Verified extractions pre-exam
- Processed/parsed extractions
- Generated digital report
- Preserved digital report to Blu-Ray disc (DEPG03)
- Verified extractions post-exam

Findings include the following:

- | | |
|-------------------------|----------------------|
| • Make | Samsung |
| • Model | SM-T510 |
| • S/N | R52N10V705X |
| • Bluetooth device name | Deena's Galaxy Tab A |
| • OS Version | Android |

305D-PG-3501933

270118

Page 3 of 14

- User accounts include:
 - Bugman25177@gmail.com eBay
 - Password: imaxxpro006
 - Bugman25177@gmail.com HBOMAX
 - Password: pizza25177
 - dgriffith919@gmail.com
 - sptzmama40@yahoo.com

A report was generated and preserved on a Blu-Ray disc labeled DEPG03.

Item07 - Seagate hard drive, Model ST5000DM002, S/N S2ABSTRW

The following processes were performed:

- Physically examined submitted evidence
- Submitted request for repair

A request was submitted to Operational Technology Division – Digital Forensic Analysis Unit – Mission Support and Data Recovery Program (MSDRP). MSDRP advised that the drive had extensive physical damage to the platters and no data could be recovered.

Item08 - Seagate hard drive, Model ST31000528AS, S/N 9VP6WVVT

The following processes were performed:

- Reviewed legal authority
- Physically examined submitted evidence
- Utilized write protection on original evidence prior to imaging
- Created an image to forensically clean media and MD5 hash verified
- Obtained hardware information
- Recovered active files, deleted files, file slack and drive free space
- MD5 hashed each file, file signature verification, full text index
- Staged for Case Agent Investigative Review (CAIR)
- Created digital report with selected items (DEPG04)
- Verified image files post-exam

The drive was not contained within a computer system. Therefore, no system date/time was obtained.

Hardware/Partition Information

Item08 contained the following hardware/partition information:

Partition	Label	File System	Size
Partition 1	Unlabeled	NTFS	953,859 MB

No operating system files were identified on this device.

305D-PG-3501933

270118

Page 4 of 14

During review, 115 items were marked as CSAM. An additional 56 items were marked as Child Exploitation. The items were found in the following locations:

	Files	Thumbnails
/transfer files/bloggie stuff/phone backup 12511/dcim/.thumbnails		
Child Exploitation – Pre-Pubescent		1
CSAM – Pre-Pubescent		1
/transfer files/save files/.thumbnails		
Child Exploitation		1
/transfer files/save files/AAA/phone fn/		
Child Exploitation – Pre-Pubescent	4	
CSAM	2	
CSAM – Pre-Pubescent	25	
/transfer files/save filesaq/save files 1/dcim/.thumbnails		
Child Exploitation		20
Child Exploitation – Pre-Pubescent		17
CSAM		6
CSAM – Pre-Pubescent		43
CASM – Pre-Pubescent – Touching		4
/transfer files/save filesaq/save files 1/dcim/Camera/		
Child Exploitation	10	
Child Exploitation – Pre-Pubescent	3	
CSAM	3	
CSAM – Pre-Pubescent	20	
CSAM – Pre-Pubescent – Touching	2	
/transfer files/save filesaq/save files 1/dcim1/100MEDIA/		
CSAM – Pre-Pubescent	1	
/transfer files/stuff 0002/phone files/dcim/.thumbnails		
CSAM – Pre-Pubescent		4
/transfer files/stuff 0002/phone pics/		
CSAM – Pre-Pubescent	4	
Total Bookmarked	74	97

A report was generated and preserved on a CD labeled DEPG04.

Item14 – Samsung mobile device, Model SM-G970U (Galaxy S10e), S/N R58M34SKCKW, IMEI 352066102864183

The following processes were performed:

- Reviewed legal authority
- Isolated device
- Physically examined device

305D-PG-3501933

270118

Page 5 of 14

GRIFFITH-000227

- Extracted data from device with advanced method
- Verified extractions pre-exam
- Processed/parsed extractions
- Generated digital report
- Preserved digital report to SanDisk 128 GB thumb drive (DEPG01)
- Verified extractions post-exam

Findings include the following:

- Make Samsung
- Model SM-G970U (Galaxy S10e)
- S/N R58M34SKCKW
- IMEI 352066102864183
- Recovered passcode (pattern) 1>2>4>5>7>8>9>6>3
- User accounts include:
 - 3044444129
 - Dancer25177
 - dancer25177@gmail.com
 - lrae25177@gmail.com
 - zmw dancer@gmail.com

A report was generated and preserved on a SanDisk 128 GB thumb drive (DEPG01).

Item17 - LG mobile device, Model LM-V600 (V60 ThinQ 5G), IMEI 353271112019922, S/N 008KPLC0121792

The following processes were performed:

- Reviewed legal authority
- Isolated device
- Physically examined device
- Locked with unknown pattern lock
- Submitted EDAU Request

Findings include the following:

- Make LG
- Model LG-V600TM (V60 ThinQ 5G)
- S/N 008KPLC0121792
- IMEI 353271112019922

Attempts to bypass the lock were unsuccessful. A request was made to Electronic Device Analysis Unit for assistance. As of this date, the request is pending.

Item21 - Samsung mobile device, Model SM-G935A (Galaxy S7 edge), S/N R38H30ZQP4P; IMEI 355503071207538; containing SIM Card ICCID 89014104271474364335

The following processes were performed:

- Reviewed legal authority
- Isolated device
- Physically examined device
- Extracted data from SIM card
- Extracted data from device with advanced method
- Verified extractions pre-exam
- Processed/parsed extractions
- Generated digital report
- Preserved digital report to Blu-Ray disc (DEPG02)
- Verified extractions post-exam

Findings include the following:

- Make Samsung
- Model SM-G935A (Galaxy S7 Edge)
- S/N R38H30ZQP4P
- IMEI 355503071207538
- SIM Card ICCID 89014104271474364335
- IMSI 310410147436433
- MSISDN 3043892804
- User accounts include:
 - Bill Griffith (Hangouts)
 - bugman25177@gmail.com (Bill Griffith)

No passcode was in use on this device.

This device contained seven (7) files tagged as possible child exploitation. All seven (7) files were found in userdata (ExtX)/Root/data/com.google.android.gms/files/downloads/.

A report was generated and preserved on a Blu-Ray disc (DEPG02).

Item24 - Dell laptop computer, Model Inspiron 3542, S/N 8ZQZ532 (HGST hard drive, Model HTS547575A9E384, S/N 130914J21400K4KV4N1B)

The following processes were performed on QPG24 and/or QPG24_1:

- Reviewed legal authority
- Physically examined submitted evidence
- Utilized write protection on original evidence prior to imaging
- Created an image to forensically clean media and MD5 hash verified
- Obtained hardware information

305D-PG-3501933

270118

Page 7 of 14

- Recovered active files, deleted files, file slack and drive free space
- MD5 hashed each file, file signature verification, full text index
- Reviewed selected registry information
- Staged for CAIR
- Created digital report with selected items (DEPG05)
- Verified image files post-exam

Hardware/Partition Information

Item24 contained the following hardware/partition information:

Partition	Label	File System	Size
Partition 1	EXP	FAT32	500 MB
Partition 2	DIAGS	FAT32	40 MB
Partition 3	Microsoft Reserved	Microsoft Reserved	128 MB
Partition 4	WINRETOOLS	NTFS	750 MB
Partition 5	OS	NTFS	704,692 MB
Partition 6	Unlabeled	NTFS	947 MB
Partition 7	PBR Image	NTFS	8,343 MB

System Information

The Operating System was identified as Windows 10 Home and was last updated on March 8, 2021. The original installation was Windows 8.1 and was installed on 03/11/2015. The registered owner was "bugman25177@gmail.com". The Microsoft account (Internet User Name) was also identified as "bugman25177@gmail.com".

References to "TorrentsData" were identified. The laptop utilized a password of "imaxxpre006". The system date/time matched the actual date/time.

During review, 245 items were marked as CSAM. An additional 1,916 items were marked as Child Exploitation. The items were found in the following locations:

	Files	Thumbnails
/Users/bugma_000/AppData/Local/Microsoft/Windows/Explorer/thumbnailcache_256.db/		
CSAM – BDSM – Pre-Pubescent		2
CSAM – Pre-Pubescent		115
CSAM – Pre-Pubescent – Touching		8
Child Exploitation – Pre-Pubescent		622
/Users/bugma_000/AppData/Local/Microsoft/Windows/Explorer/thumbnailcache_48.db/		
CSAM – BDSM – Pre-Pubescent		2
CSAM – Pre-Pubescent		83
CSAM – Pre-Pubescent – Touching		9

Child Exploitation – Pre-Pubescent		472
/Users/bugma_000/AppData/Local/Microsoft/Windows/Explorer/thumbnailcache_768.db/		
Child Exploitation – Pre-Pubescent		1
/Users/bugma_000/Desktop/Desktop folder/junk/100MEDIA/STUFF/phone pics 4-9-15/Thumbs.db/		
Child Exploitation – Pre-Pubescent		2
/Users/bugma_000/Desktop/Desktop folder/old phone backup 282021/Download/		
Child Exploitation – Pre-Pubescent	2	
/Users/bugma_000/Desktop/Desktop folder/stuff0002/Deenas phone stuff/2015-11/		
Child Exploitation – Pre-Pubescent	3	
/Users/bugma_000/Desktop/save files/bills phone backup 1172021/Album 1001/		
CSAM – Pre-Pubescent	13	
Child Exploitation – Pre-Pubescent	152	
/Users/bugma_000/Desktop/save files/bills phone backup 1172021/TorrentsData/Sandra Model_AMS 049 (Rare Extended 168 pics) (1)/Sandra Model_AMS 049 (Rare Extended 168 pics)/Thumbs.db/		
Child Exploitation – Pre-Pubescent		168
/Users/bugma_000/Desktop/save files/bills phone backup 1172021/TorrentsData/Sandra Model_AMS 049 (Rare Extended 168 pics).rar/Sandra Model_AMS 049 (Rare Extended 168 pics)/		
CSAM – Pre-Pubescent	13	
Child Exploitation – Pre-Pubescent	152	
/Users/bugma_000/Desktop/save files/bills phone backup 1172021/TorrentsData/Sandra Model_AMS 049 (Rare Extended 168 pics).rar/Sandra Model_AMS 049 (Rare Extended 168 pics)/Thumbs.db/		
Child Exploitation – Pre-Pubescent		168
/Users/bugma_000/Desktop/save files/bills phone backup 1172021/TorrentsData/Sandra Model_AMS 049 (Rare Extended 168 pics)/Sandra Model_AMS 049 (Rare Extended 168 pics)/Thumbs.db/		
Child Exploitation – Pre-Pubescent		168
/Users/bugma_000/Desktop/save files/new phone sd card back up 282021/Album 1/		
Child Exploitation – Pre-Pubescent	6	
Total Bookmarked	341	1820

305D-PG-3501933

270118

Page 9 of 14

GRIFFITH-000231

A report was generated and preserved on a CD labeled DEPG05.

Screenshots of what appear to be a Samsung device were located on this computer. Multiple applications indicating the use of file sharing and/or torrent browsers were noted. These applications include DropBox, Frostwire, One Drive, Onion Browser, TorBrowser, WeTorrent, Orbot and Orweb. Applications indicating wiping/erasing were also noted. These include Secure Eraser and SecureWipe. Applications indicating advanced file access were also noted. These include DiskDigger, FileChef and Recover Deleted Data. In addition, applications with file sharing features were noted. These include Discord, MeWe, My Cloud OS 3, Signal, Snapchat, TextFree, Twitter, Facebook Messenger, Facebook Messenger Kids and Zello.

Artifacts identifying DropBox were identified. However, no user data could be identified. Artifacts identifying OneDrive were also identified. A OneDrive account for "bugman25177@gmail.com" was identified.

Item25 - CyberPower desktop computer, Model C Series (Western Digital SATA SSD, Model WDS240G2G1A, S/N 202014A00DAD and Western Digital SATA SSD, Model WDS240G2G1A, S/N 202014A00DAD)

The following processes were performed on QPG25 and/or QPG25_1:

- Reviewed legal authority
- Physically examined submitted evidence
- Utilized write protection on original evidence prior to imaging
- Created an image to forensically clean media and MD5 hash verified
- Obtained hardware information
- Recovered active files, deleted files, file slack and drive free space
- MD5 hashed each file, file signature verification, full text index
- Reviewed selected registry information
- Staged for CAIR
- Created digital report with selected items (DEPG06)
- Verified image files post-exam

Hardware/Partition Information

Item25_1 contained the following hardware/partition information:

Partition	Label	File System	Size
Partition 1	SYSTEM	FAT32	100 MB
Partition 2	Microsoft Reserved	Microsoft Reserved	16 MB
Partition 3	Windows	NTFS	228,319 MB
Partition 4	Recovery	NTFS	500 MB

System Information

The Operating System was identified as Windows 10 Home and was last updated on May 29, 2021. This date also appears to be the original installation date. The Microsoft account (Internet User Name) was also identified as "bugman25177@gmail.com". A profile was identified for "bugma (Bill Griffith)".

A review of Recent Docs identified links to the following:

- LS Little Guests 037.Ink
- Removable Disk (Z).Ink
- Removable Disk (Z) (2).Ink
- USB Drive (F).Ink
- USB Drive (F) (2).Ink
- backup 1 11 2022.Ink
- Torrents.Ink
- LS-island.Set.017.by_zic.Ink

During review, 21,774 thumbnails were marked as Child Sexual Abuse Material or Child Exploitation material. The items were found in the following locations:

	Files	Thumbnails
/Users/bugma/AppData/Local/Microsoft/Windows/Explorer/thumbcache_1280.db/		
Child Exploitation		1
Child Exploitation – Pre-Pubescent		5
/Users/bugma/AppData/Local/Microsoft/Windows/Explorer/thumbcache_256.db/		
CSAM – BDSM – Pre-Pubescent		27
CSAM		197
CSAM – Pre-Pubescent		1,187
CSAM – Pre-Pubescent – Touching		56
Child Exploitation		884
Child Exploitation – Pre-Pubescent		5,431
/Users/bugma/AppData/Local/Microsoft/Windows/Explorer/thumbcache_48.db/		
CSAM		4
Child Exploitation		28
Child Exploitation – Pre-Pubescent		318
/Users/bugma/AppData/Local/Microsoft/Windows/Explorer/thumbcache_768.db/		
Child Exploitation		3
Child Exploitation – Pre-Pubescent		5

305D-PG-3501933

270118

Page 11 of 14

/Users/bugma/AppData/Local/Microsoft/Windows/Explorer/thumbcache_96.db/		
CSAM – BDSM		2
CSAM – BDSM – Pre-Pubescent		3
CSAM		60
CSAM – Pre-Pubescent		1,108
CSAM – Pre-Pubescent – Touching		13
Child Exploitation		588
Child Exploitation – Pre-Pubescent		11,852
/Users/bugma/AppData/Local/Packages/microsoft.windowscommunicationsapps_8wekyb3d8bbwe/LocalState/Files/S0/3/Attachments/		
CSAM – Pre-Pubescent		
Child Exploitation – Pre-Pubescent		2
Total Bookmarked	0	21,774

The following processes were performed on QPG25_2:

- Reviewed legal authority
- Physically examined submitted evidence
- Utilized write protection on original evidence prior to imaging
- Created an image to forensically clean media and MD5 hash verified
- Obtained hardware information
- Recovered active files, deleted files, file slack and drive free space
- MD5 hashed each file, file signature verification, full text index
- Review conducted
- Drive appears to be unused
- Verified image files post-exam

Hardware/Partition Information

Item25_2 contained the following hardware/partition information:

Partition	Label	File System	Size
Partition 1	Microsoft Reserved	Microsoft Reserved	15 MB
Partition 2	New Volume	NTFS	953,852 MB

This drive appears to be unused. No further examination was conducted.

Definitions/Explanations:

An IMEI (International Mobile Equipment Identity) and an MEID (Mobile Equipment Identifier) are both used to identify mobile devices. An IMEI is used on GSM (Global System for Mobile Communication) and an MEID is used on CDMA (Code-Division Multiple Access).

Integrated Circuit Card Identifier (ICCID) is a unique serial number for the SIM card. It is stored in the SIM card and also printed on the card.

International Mobile Subscriber Identity (IMSI) is a unique number associated with all Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) network mobile phone users used for identifying a GSM subscriber. The IMSI is stored in the Subscriber Identity Module (SIM) inside the phone and is sent by the phone to the appropriate mobile network.

Mobile Station International Subscriber Directory Number (MSISDN) is a number used to identify a phone internationally.

A Message Digest 5 (MD5) hash is an algorithm applied to digital media or files generating a unique signature in the form of a hexadecimal number.

The Known File Filter (KFF) compares file hashes against a database of hashes for known files. The purpose of the KFF is to eliminate unimportant files (known software installation files) or to identify alert files.

File signature verification is a comparison of the file headers to a database of known file types. The file header is the initial string of characters in a file, unique to a given file type. Unlike the file extension, the file header is difficult to change in an attempt to hide files.

Full text indexing is the building of an index which includes all text on the media regardless of where it is located on the media. This index is used to allow subsequent key word searches to be performed very quickly.

The Windows Registry is the centralized configuration database used to help Windows control hardware, software, the user's environment and the appearance of the Windows interface.

Derivative Evidence (DE)/Copies:

An integral part of this report is the digital extraction reports (DEPG01 through DEPG06). These results contain a home page (main.html) at the root of the disc. Double-clicking the main.html file should bring up the reports.

The results can also be reviewed by utilizing OpWAN.

- DEPG01 SanDisk 128 GB thumb drive containing results of examination and files for review from Item14
- DEPG02 Blu-Ray disc (25 GB) containing results of examination and files for review from Item21
- DEPG03 Blu-Ray disc (25 GB) containing results of examination and files for review from Item02
- DEPG04 CD containing results of examination and files for review from Item08

DEPG05 CD containing results of examination and files for review from Item24
DEPG06 DVD containing results of examination and files for review from Item25_1
DEPG07 LTO6 cartridge containing archive of image files
DEPG08 LTO5 cartridge containing archive of processing and examination results

Disposition of Items:

All original evidence was returned to the Evidence Control Technician. All derivative evidence (DEPG01 through DEPG08) was submitted to the Evidence Control Technician to be entered as new 1B items. Notes will be maintained in the 1A section of the CART Control file.

Examiner: 
Melinda C. Cash

Pittsburgh Division
Charleston, WV Resident Agency
Computer Analysis Response Team